Agentschap voor Innovatie door Wetenschap en Technologie

IWT

SBO Security and Privacy for Online Social Networks

Document type	Report
Title	Guidelines for Privacy-Friendly Default Settings
Deliverable Number	D9.6.5
Authors	Valerie Verdoodt and Brendan Van Alsenoy
Dissemination level	Internal
Preparation date	December 2014
Version	1.0

The IWT SBO SPION Project

Nr.	Participant name	Country	Department	Participant role
1	KU Leuven	BE	COSIC/ESAT	Coordinator
2	KU Leuven	BE	DISTRINET	Partner
3	KU Leuven	BE	DTAI	Partner
4	KU Leuven	BE	ICRI	Partner
5	Vrije Universiteit Brussel	BE	SMIT	Partner
6	Univerity of Ghent	BE	OWK	Partner
7	Carnegie Melon University	USA	Heinz	Partner

Contributors

	Name	Organisation
1	Valerie Verdoodt	ICRI, KU Leuven, iMinds
2	Brendan Van Alsenoy	ICRI, KU Leuven, iMinds
3	Rula Sayaf	Distrinet, KU Leuven, iMinds
4	Alessandro Acquisti	CMU

TABLE OF CONTENTS

1. INTRODUCTION

Privacy settings allow users to exercise a certain degree of control over who can access the information they share through Online Social Networks (OSNs).[1] Unfortunately, research has shown that many users do not bother to change their privacy settings or remain unaware of the actual audiences with whom their data is shared. In addition, OSNs are corporations with a commercial imperative to set the default to obtain as much personal data as possible.[2] Consequently, even if the user selects certain privacy settings, the website's default settings might still operate beyond the users' expectations.[3]

Privacy-friendly default settings have been put forth as a way to alleviate part of the burden placed on individuals.[4] Such settings have pre-selected values which are designed to respect the users' privacy and that no further actions are required from them to be sufficiently protected.[5] The concept of "privacy by default" has also been recognised by the European Commission in their proposal for a general Data Protection Regulation.[6] Once the Regulation comes into force, the OSN provider will have to implement both safeguards into the design of the platform as well as privacy-friendly default settings.[7]

The legal framing of default settings has already been analysed extensively in a previous deliverable.[8] The objective of this deliverable is to provide more practical guidelines for the appropriate configuration of privacy-friendly default settings. It starts by summarizing the relevance of default settings from a behavioural economics perspective. Next, an inventory is made of the current default settings offered by main OSN providers. The guidelines themselves will cover 6 main elements, namely: (1) awareness and active choice; (2) granularity; (3) audience visibility; (4) simplicity; (5) user expectations and (6) proportionality.

---

[1] I. Byrnside, "Six Clicks of Sepparation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants", Vanderbilt Journal of Entertainment and Technology Law, 2008, 10, as cited by P. Lambert, *Social Networking: Law, Rights and Policy*, Dublin, Clarus Press, 3 April 2014, 105.
[2] P. Lambert, *Social Networking: Law, Rights and Policy*, Dublin, Clarus Press, 3 April 2014, 107.
[3] *Idem*.
[4] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 3, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.
[5] Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosystem*, October 2012, 18, http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf; J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 24.
[6] Article 23 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011.
[7] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 30.
[8] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 23.

2. THE RELEVANCE OF DEFAULT SETTINGS

Privacy blunders happen every day. Very often, these blunders are the result of poorly configured privacy settings. In the context of OSNs, there are several factors which may influence users' configuration of privacy settings, including:

- pre-existing default settings;
- incomplete information;
- cognitive and behavioural biases; and
- invisibility of audiences.

2.1. The "power of default"

Behavioural economics research has shown that many individuals do not bother to change their privacy settings.[9] The Article 29 Working Party has likewise stressed that only a minority of the OSN users that have signed up to a service will actually change their default settings.[10] One reason for this could be that users are simply not aware of the possibility to tweak their settings.[11] Other possible explanations include motivational limitations and time constraints.[12]

2.2. Incomplete information

Privacy choices are often affected by incomplete information.[13] In an OSN environment, there are information asymmetries which hinder individuals' privacy decision-making as only a subset of parties has knowledge of the relevant information.[14] The OSN provider is the only party that fully grasps the amount of data that is being collected, for which purposes and which third parties have access.[15] Thus, many times,

---

[9] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy*, vol3, No 1, January/February 2005, 27; S. Livingstone, "Taking Risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression", *New Media and Society* 10 (2008).

[10] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[11] A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook" in G. Danezis, P. Golle (eds.), *Privacy-Enhancing Tech.: 6Th Int'L Workshop,* vol. 36 (2006), http://privacy.cs.cmu.edu/dataprivacy/ projects/facebook/facebook2.pdf; S. Livingstone, "Taking Risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression", *New Media and Society* 10 (2008).

[12] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy*, vol3, No 1, January/February 2005, 27.

[13] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 1-2.

[14] I. Adjerid, A. Acquisti, L. Brandimarte, G. Loewenstein, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, *Symposium on Usable Privacy and Security (Soups) 2013*, 24-26 July 2013, Newcastle, UK, 2; A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 2.

[15] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy*, vol3, No 1, January/February 2005, 27; R. Balebako, P.G. Leon, H. Almuhimendi, P.G. Kelly, J. Mugan,

users do not know with whom and more importantly for which purpose their data is being used and how this may affect them. Transparent privacy policies that provide clear information can help reduce information asymmetries to some extent. Nevertheless, their practical implementation is such that many users fail to derive meaningful information from them.[16]

Incomplete information leads to increased complexity of privacy decision-making. As stated by ACQUISTI and GROSSKLAGS, "*the complexity of the privacy decision environment leads individuals to arrive at highly imprecise estimates of the likelihood and consequences of adverse events, and altogether ignore privacy threats and modes of protection"*.[17] As a result, the actual outcome of user choices often does not reflect their expectations.

2.3. Cognitive and behavioral biases

Even if individuals were to have complete information, they would be faced with other factors complicating their privacy choices. It has been argued that individuals can only rationalise to a certain extent about data which is available to them (i.e., "bounded rationality").[18] Finding information costs time and energy, especially in relation to complex decisions like the protection of personal data. Bounded rationality limits OSN users' ability to collect and process all relevant information. Given that the tangible and intangible consequences of privacy decisions are difficult to estimate, individuals rely on heuristics and draw inaccurate conclusions from past choices.[19] In addition, individuals are inclined to be overconfident and tend to underestimate risks, especially when they do not immediately experience consequences.[20] Finally, individuals are susceptible to the way in which information is presented to them ("framing"), as well as to the specific timing of the information provision.[21] HELBERGER for example, argues that individuals tend

---

A. Acquisti, L.F. Cranor and N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", *CHI 2011*, May 7 - 12 2011, Vancouver, BC, Canada, 1.

[16] See also B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", International Review of Law, Computers & Technology 2013, p. 5 et seq.

[17] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 3.

[18] M.A. Eisenberg, "The Limits of Cognition and the Limits of Contract", *47(2) Stanford Law Review*, 1995, 214; H.A. Simon, "Models of bounded rationality. Trustme: Anonymous management of trust relationships in decentralize P2P systems", in N. Shahmehri, R.L. Graham & G. Caronni (Eds.), *Peer-to-peer computing*, Washington DC, USA: IEEE Computer Society, 142-149; E. Wauters, E. Lievens, P. Valcke, D1.2.4: A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment', 19 December 2013, 8, www.emsoc.be.

[19] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 6; A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making", *IEEE Security & Privacy*, vol3, No 1, January/February 2005, 27; I. Adjerid, A. Acquisti, L. Brandimarte, G. Loewenstein, "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, *Symposium on Usable Privacy and Security (Soups) 2013*, 24-26 July 2013, Newcastle, UK, 2.

[20] E. Wauters, V. Donoso and E. Lievens, "Why are Terms of Use so difficult to understand? Reflections on how to optimize transparency for users in Social Networking Sites", EuroCPR, Brussels, 24-25 March 2014, 2.

[21] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, 7; E. Wauters, V. Donoso, E. Lievens and P. Valcke, "Re-designing & re-

to forget information when it is not yet relevant to them (e.g., the beginning of the signing-up process), and therefore posits that information should instead be provided in the right portions and in the right context.[22] These cognitive and behavioural biases affect OSN users' decision making and causes them to deviate from so-called rational privacy decisions.[23]

2.4. Invisibility of audiences

A fourth important element which influences the decision-making of OSN users is the nature of OSNs. Its specific characteristics, like the invisibility of audiences, have been designed to increase the sharing of information.[24] Research has shown that, for instance, Facebook users cannot accurately estimate who is actively following them on the OSN.[25] Due to this lack of social transparency, OSN users are not sufficiently aware of the possible consequences of their online sharing habits. In other words, they might be sharing more information than they would if they were actually aware of who is watching their online behaviour.

---

modeling Social Network terms, policies, community guidelines and charters: Towards a user-centric approach", EMSOC Project, 31 March 2014, 34, available on www.emsoc.be.

[22] N. Helberger, "Form Matters: Informing Consumers Effectively, 15 November 2013, Amsterdam Law School Research Paper No. 2013-71, 24 available on http://ssrn.com/abstract=2354988.

[23] A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us About Privacy", presented as Keynote Paper at ETRICS 2006, p. 5 et seq.

[24] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 20.

[25] M.S. Bernstein, E. Bakshy, M. Burke and B. Karrer, "Quantifying the Invisible Audience in Social Networks", *CHI 2013*, April 27–May 2, 2013, Paris, France, 2.

3. INVENTORY OF CURRENT DEFAULT SETTINGS

Privacy settings are access control mechanisms (hereinafter "ACM") which allow users to decide who can access their "user data".[26] An ACM is the formalisation of how policies are composed based on a specific set of features in the system, regulating and authorising access to data.[27] They are a means of diminishing privacy and security risks of unauthorised access to the data in information systems. Essentially, OSN users have the possibility to select their preferred privacy settings and each of these settings define which group of people receives access to the information shared on that person's profile. They can either select an audience from a predefined set of groups (e.g., Friends, Friends of Friends, only me, Public), or customise their own audience. The table below provides an overview of the possible settings of a selection of social networks.[28]

Social Network	Default settings regulating access by users	Other possible settings regulating access by users	Interesting to note	Default settings regulating access by OSN providers	Default settings regulating access by third parties
Facebook	Friends (for new users[29]). However, certain "basic" profile information is always publicly available (name, profile and cover pics, networks, gender, username and user id).[30]	Public, Friends only, Friend of friends, custom.	Users are allowed to define the audience for each post separately. When new users post something for the first time, they can select their audience for that particular post, if they don't select anything their info is shared with friends only. If they do change the audience for that post, for instance to public, this change will be sticky, which means	Access to all user data. These settings are wired-in so they can't be changed. These data may be freely shared within the family of companies that are part	User data may be used by the following third parties: 1. Advertising, measurement and analytics services in "non-personally identifiable form".[32] 2. "We transfer information to vendors, service providers, and other partners who globally

[26] This includes both basic profile information and additional information that the OSN user adds to his or her profile.
[27] R. Sayaf & D. Clarke, "Access Control Models For Online Social Networks", 2, in L. Caviglione et al. (eds), *IGI Global*, 2012 accessible at https://lirias.kuleuven.be/bitstream/123456789/373507/1/ACMs%20in%20OSNs.pdf.
[28] This table was last updated on 5 December 2014.
[29] For existing users this used to be public.
[30] Facebook, *Information we receive and how it is used*, last visited 15 October 2014, www.facebook.com. This public information can also show up when someone does a search on Facebook or on another search engine, see https://www.facebook.com/help/203805466323736.
[32] https://www.facebook.com/about/privacy/update.

			that future posts will also be shared publicly.	of Facebook.[31]	support our business"[33] This setting is wired-in, so it cannot be changed.
Twitter	Public	Private (tweets will only be available to approved followers).	Users with a private account cannot answer to tweets of people that are not following them.	Access to all data related to the user.	Service providers, sellers of goods and services, affiliates, advertisers (public info).
Instagram	Public	Private (approved followers)	Posts can't be set to private from a desktop computer at this time. Find friends: users can choose to search contacts through their contact list/other OSNs, to which Instagram would then receive access.	Access to all data related to the user.	User data may be shared with affiliates, service providers, third-party advertising companies (wired-in).[34]
Snapchat	My Friends	Everyone, Custom (as regards who can view my story, not who can send me snaps).	Snapchat may "*collect information from your device's phonebook and photos*" but only with the user's consent. Additionally, Snapchat may share information about a user with other users who have this person's phone number in their device phonebook. "*For instance, when you use Find Friends, we may share your username and name with other users who use Find Friends and have your phone number in their device phonebook.*"	Access to: basic profile information (e.g., password, username, date of birth, email), usage info (e.g., time, date, sender, recipient of a message), content info[35], device info, device phonebook and photos, location info,	1. Analytics advertising services provided by third parties: "We may let other companies use cookies, web beacons, and other technologies on Snapchat. These companies may collect information about how you use the Services and other websites and online services over time and across different services. The information collected may include unique

[31] Including: Facebook Payments Inc, Atlas, Instagram LLC, Mobile Technologies Inc., Onavo, Parse, Moves, Oculus, LiveRail, WhatsApp Inc., https://www.facebook.com/help/111814505650678.

[33] Facebook does not provide a list of data that might be shared with these third parties, https://www.facebook.com/about/privacy/update.

[34] http://instagram.com/about/legal/privacy/#section3.

[35] In this regard, Snapchat does not guarantee that messages are deleted within a specific timeframe, data and states that "*even after we've deleted message data from our servers, that same data may remain in backup for a limited period of time*". Furthermore, Snapchat admits in its privacy policy that there "*there may be ways to access messages while still in temporary storage on recipients' devices or, forensically, even after they are deleted*.", see https://www.snapchat.com/privacy.

				info collected by cookies, website log info.	device identifiers, device manufacturer and operating system, IP address, browser type, pages viewed, session start/stop time, links clicked, and conversion information. This information may be used to, among other things, analyze and track data, determine the popularity of certain content, and better understand your online activity. Data may be shared with vendors, consultants and other service providers who need access to such information to carry out work on behalf of snapchat" (wired-in).[36]
Ello	Public[37]	/	Ello is invitation only, therefore potential users must request an invitation. Users can opt-out of the use of Google Analytics and Ello also respects "Do not track" browser settings.	Access to general, non-identifiable information about what pages you access, your general geographic location (e.g., a city, but not a street address), the device you are using, an anonymized version of your IP address, the	Google Analytics (but users have the possibility to opt-out). "We may share your information, including personal information, with third parties under several circumstances, including (1) if you tell us it is OK to do so (2) if we believe that we need to do so to comply with applicable law or legal obligations

[36] Snapchat does not clarify what kind of data is being shared https://www.snapchat.com/privacy.
[37] This is the only option Ello provides for its users. "Users should assume that anything you post or upload on the Site other than private messages will be accessed by the public." https://ello.co/wtf/post/privacy.

				address of web sites that refer you to the site, email address and UserID.	(3) if we contract with a third party service provider to offer services for you — for example, with a credit card processing company if you decide to buy something through the Site. Ello does not have any affiliated companies right now. But if we do in the future, we may share information with them, too.[38]

[38] https://ello.co/wtf/post/privacy.

4. GUIDELINES FOR PRIVACY-FRIENDLY DEFAULT SETTINGS

4.1. Awareness and active choice

Only a limited number of OSN users changes their default settings or is even aware that these settings can be tweaked.[39] Awareness is the first step towards making informed privacy decisions. Therefore, it is important that OSN providers look at ways to increase the level of awareness of the users of their services. This can be achieved, for instance, by providing sufficient information about the default settings and other possible choices when they sign up for the service, or when they decide to change them.

Active choice can further enhance user awareness. Active choice implies that users must "*freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts*".[40] In other words, OSN providers should wait for an affirmative action of the user before sharing his or her information to a broader audience than just "friends" or "connections". Active choice also implies that no changes should be made to default settings without the user's affirmative consent. Mere notification of changes is not enough.[41]

Privacy-friendly

- ✓ When users join the OSN, they are clearly informed about the different functionalities of their privacy settings and actively stimulated to customise them.
- ✓ Require an affirmative action of the user for every change in settings.

Not privacy-friendly

- × Implementing changes in settings without the users' explicit consent.
- × Changing the default from private to public and only notifying users after the fact.

4.2. Granularity

Granularity of privacy settings determines how much control a user may exercise over the sharing of his or her personal data.[42] Granular settings allow OSN users to specify what parts of their user data should be accessible to others.[43] In practice, many OSN providers offer only two options for OSN users: they can either choose to make their

---

[39] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 15.

[40] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[41] See also A. Kuczerawy and F. Coudert, "Privacy Settings in Social Networking Sites: Is It Fair?" in S. Fischer-Hübner et al. (Eds.), Privacy and Identity 2010, IFIP AICT 352, 235.

[42] R. Balebako, P.G. Leon, H. Almuhimendi, P.G. Kelly, J. Mugan, A. Acquisti, L.F. Cranor and N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", *CHI 2011*, May 7 - 12 2011, Vancouver, BC, Canada, 3.

[43] The Oxford Dictionary defines granularity as "the scale or level of detail in a set of data", http://www.oxforddictionaries.com/definition/american_english/granularity.

profile information publicly available or keep it entirely private.[44] Such an absence of further granularity might urge users to make more information visible to public than they would otherwise.[45] On the other hand, it should be taken into account that an overabundance of choices might bury the important settings.[46] For instance in Facebook's new 'privacy basics' information[47], there are several granular settings regulating access by other OSN users, which might confuse users. To set the right level of granularity, a balancing exercise is necessary.

Privacy-friendly

- ✓ Make sure the privacy settings provide a sufficient level of granularity.
- ✓ Allow and stimulate customised settings, whereby users can easily and exactly select a specific audience for their posts and other parts of their profile.[48]
- ✓ Allow users to exercise control over the use of their personal information by the OSN provider and third parties.
- ✓ Enable users to exercise some control over the information about them that is being posted by fellow users (e.g., by requiring prior approval for a photo tag by default).

Not privacy-friendly

- × Present users with an all-or-nothing choice in relation to the access by other OSN users and third parties.
- × Only mention privacy risks resulting from other consumers accessing the information (without mentioning risks resulting from the collection and use by other third parties).[49]
- × Offering an overabundance of choices regulating access by other users as this might confuse users

---

[44] For instance ,Twitter and Instagram only provide those two options. The platform Ello does not even provide an option for its users, as the public setting is wired-in.
[45] R. Balebako, P.G. Leon, H. Almuhimendi, P.G. Kelly, J. Mugan, A. Acquisti, L.F. Cranor and N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", *CHI 2011*, May 7 - 12 2011, Vancouver, BC, Canada, 3.
[46] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 22.
[47] Facebook Privacy Settings and Tools, last consulted on 8 December 2014, https://www.facebook.com/settings?tab=privacy.
[48] Facebook for instance allows this possibility for each post, however it does not for other elements like a specific picture in an album.
[49] For instance, Facebook, Google+.

4.3. Audience visibility

OSN users often underestimate their actual audience when disclosing personal information on their profiles.[50] One way to increase 'social transparency' is by improving audience visibility. [51] Tools such as Freebu[52] make it easier to see which people belong to which groups. Another way to increase audience visibility is to display to the user a subset of the contacts who will be able to view certain content before he or she posts it. Such "social transparency" tools can encourage users to take a more cautious approach to online information sharing, as they are forced to think about who is actually watching or listening.

Privacy-friendly

- ✓ Provide indications of how many people can really view a picture or read a statement.
- ✓ Facilitate grouping and audience management (e.g., Freebu).

Not privacy-friendly

- × Offering an abundance of choices regulating access by other users to distract users from the fact that there are no options to regulate access by the OSN provider or third parties.

4.4. Simplicity

Configuring privacy settings should be easy. A simple, logical and comprehensive privacy pane is necessary, so that OSN users can easily determine how their settings will impact the visibility of their information. At the same time, it is also important to provide users with the right information and choice at the moment of decision-making. Users should therefore be able to customize settings at the moment of information sharing.

Privacy-friendly

- ✓ Make the privacy pane as simple and logical as possible and provide understandable explanations.
- ✓ Enable configuration of the settings at the moment of content sharing.

---

[50] In most OSNs the only signs of interaction are likes or comments. See M.S. Bernstein, E. Bakshy, M. Burke and B. Karrer, "Quantifying the Invisible Audience in Social Networks", *CHI 2013*, April 27–May 2, 2013, Paris, France, 9.

[51] Social transparency has been defined as the availability of social meta-data surrounding information exchange. See H. C. Stuart , L. Dabbish, S. Kiesler, P. Kinnaird and R. Kang, "Social Transparency in Networked Information Exchange: A Framework and Research Question", *CSCW'12*, 11-15 February 2012, Seattle, Washington, USA.

[52] Freebu is an online application, which helps to create your own Facebook friend-lists (audience management) and offers four interactive visualisations.

Not privacy-friendly

- × Using legalese while explaining default settings.
- × Scattering settings across a myriad of pages making it difficult for individuals to configure.

4.5. User expectations and societal values

Default settings should reflect user expectations. Expectations of the OSN user should be determined on a case-by-case basis, as there is no one-size-fits-all solution. Different social networking platforms can create different expectations. For instance as regards Facebook, it could be reasonable to expect that statements or other information posted by an OSN user on his profile page, is by default shared amongst this user's friends. Conversely, a platform such as Twitter might not trigger the same expectations, as it is promoted as a public discussion forum. Similarly, if a user has opted for a restricted access profile, internal search engines should also respect this choice by default.[53]

Finally, it is important to note that when minors join OSN platforms, additional protection might be necessary. For instance, it has been argued that it would be more appropriate to, instead of defining a privacy-friendly default setting, have a privacy-friendly setting wired-in for minors (e.g., make profiles of minors only accessible to friends). [54]

Privacy-friendly

- ✓ Limiting the amount of "basic profile information" which is public by default, including the number of connections.[55]
- ✓ Restricted access profiles should remain hidden when using internal search engines. This also includes searches by specific parameters like age or location.[56]
- ✓ Profiles of minors should only be accessible to friends

---

[53] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[54] J. Ausloos, E. Kindt, E. Lievens, P. Valcke and J. Dumortier, "Guidelines for Privacy-Friendly Default Settings", *ICRI Working Paper Series*, 18 February 2013, 23.

[55] The reason for this is that in a certain social media context, for instance in the case of LinkedIn, users are actually encouraged to add as many connections as possible, as this might be beneficial in the job searching process. Consequently, information is being disclosed to more people, which might increase the risk to privacy infringements. See R. Balebako, P.G. Leon, H. Almuhimendi, P.G. Kelly, J. Mugan, A. Acquisti, L.F. Cranor and N. Sadeh, "Nudging Users Towards Privacy on Mobile Devices", *CHI 2011*, May 7 - 12 2011, Vancouver, BC, Canada, 3.

[56] Article 29 Working Party Opinion 5/2009 on online social networking, 12 June 2009, 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

Not privacy-friendly

- × Choosing an unfair default setting which causes users to unwillingly disclose personal information.[57]
- × Allowing all "basic profile information" to be public by default, without taking into account user expectations.

4.6. Don't be intrusive

Artificial intelligence ("AI") techniques, such as facial recognition and in depth content analysis, can offer considerable insights into individual's behavior. While these techniques can be used for benign purposes, they also have a substantial impact on individuals' privacy. For example: Facebook's Artificial Intelligence Research lab has recently been experimenting with software that would be able to distinguish between "drunk" and "sober" pictures. Using this technology, the OSN could warn its users and thus prevent them from uploading potentially embarrassing pictures. [58] However, one can question whether such techniques are really necessary to achieve this objective. Less intrusive nudging techniques (such as increased audience visibility or introducing a timer) may already substantially mitigate risks of reckless posting. In any event, it would seem appropriate that individuals not be subjected to such techniques by default, but only after an affirmative choice.

Privacy-friendly

- ✓ Use of non-intrusive nudging techniques (e.g., increased audience visibility).

Not privacy-friendly

- × Using facial recognition to automatically link pictures to individuals without their permission
- × Using in depth content analysis and AI without their express consent.

---

[57] For instance the FTC received a complaint against the peer-to-peer company FrostWire. According to the FTC, "*Frostwire had configured the application's default settings so that, immediately upon installation and set-up, it would publicly share users' photos, videos, documents, and other files stored on those devices*", see Facebook offers solution to end drunken posts" http://www.ftc.gov/news-events/press-releases/2011/10/peer-peer-file-sharing-software-developer-settles-ftc-charges.

[58] D. Lee, "Facebook offers solution to end drunken posts", *BBC News Technology*, 11 December 2014, accessible at http://www.bbc.com/news/technology-30432493

5. CONCLUSION

Privacy-friendly default settings can help mitigate risks of inadvertent disclosure. Nevertheless, OSN users should be clearly informed about the different functionalities of their privacy settings and actively stimulated to customize them. In absence of an affirmative choice, profile content should only be available to the user's self-selected contacts.

When creating default settings, OSN providers should first of all define the appropriate level of granularity. On the one hand, offering too little choice may lead to excessive disclosure. On the other hand, too much choice may be confusing or overwhelming. OSN providers should make privacy choices as simple intuitive as possible, both through comprehensive privacy panes and 'just-in-time' configuration.

Audience management is a challenge for many OSN users. OSN providers should therefore strive to ensure audience visibility and provide tools which help users to decide which groups of individuals should have access to which information.

Finally, OSN providers should continue to take into account users' expectations when introducing new features. While sophisticated forms of content analysis may yield new insights, they may also be seen as intrusive. Allowing individuals to choose before they are subject to new features will help keep users' expectations of privacy intact.